Healthcare
Role-Based Access Control
Task Force Charter

Version 1.1

Developed For:
The Healthcare RBAC Task Force

Developed by:
Science Applications International Corporation (SAIC)
22 July 2003

TABLE OF CONTENTS

LIST OF TABLES

1 Scope

This charter document is a high-level overview of the proposed tasks and goals to be accomplished by the Healthcare Role-Based Access Control (RBAC) Task Force (TF).

The primary goal of the Healthcare RBAC TF is to define a common, industry-wide harmonized list of healthcare work profiles and access control permissions and present them as a recommended standard to a Standards Development Organization (SDO). Targeted SDOs include the American Society for Testing and Materials (ASTM), Health Level Seven (HL7) and National Institute of Standards and Technology (NIST). The SDO would then turn the information into a proposed RBAC standard for use within the healthcare community.

The Healthcare RBAC TF will be established with representatives from large healthcare organizations, including Department of Defense (DoD) and Indian Health Service (IHS), Kaiser Permanente (KP) and Department of Veterans Affairs (VA). Other healthcare organizations may join the collaboration in the future. Additionally, the SDOs will participate as advisory members. Participating healthcare organizations will adopt and implement the Healthcare Charter via a Memorandum of Understanding (MOU) in which each organization agrees to support the RBAC effort. Additionally, each participating healthcare organization will establish its own Enterprise RBAC TF. Each Enterprise RBAC Task Force will be composed of knowledgeable individuals (health care providers, system developers, security experts, etc) as needed within that organization. Representatives from each Enterprise RBAC TF will participate in the Healthcare RBAC TF.

1.1 Business Case

"Should this person (or a person who performs this job function) typically be allowed to access this type of data?"

RBAC is critically important to the security aspects of healthcare organizations. The Healthcare RBAC TF goal is to establish a mechanism for scaleable management of user permissions in the form of a list of roles and tasks (role-based access), then provide that list to system access control and authorization services. The National Institute of Standards and Technology (NIST) defines role-based access as when: “access decisions are based on the roles that individual users have as part of an organization. Users take on assigned roles (such as doctor, nurse, teller, manager). The process of defining roles should be based on a thorough analysis of how an organization operates and should include input from a wide spectrum of users in an organization.”

RBAC products are continually evolving. Available products have advanced to support more complex issues than simple end-user authentication and password management. The complex issues include centralizing the administration for endpoint systems, administering end-users through a role-based view that allows a large population of end-users to be affected by a single system administration change (e.g., adding a new application to the workstations of all supported users), and monitoring end-user usage of sensitive applications, resources and data.

1.2 Healthcare RBAC Task Force Objectives

The objectives of the Healthcare RBAC TF are outlined below:

- Establish a Healthcare RBAC Task Force composed of individuals knowledgeable in healthcare workflow to define core roles supporting healthcare functions within healthcare organizations. The Healthcare RBAC Task Force will support the development of ANSI-standard health information roles. This task force will be composed of representatives from VA, DoD, KP and IHS.

- Adopt the RBAC Role Engineering Process document, which includes standard terms, definitions and RBAC process by the Enterprise RBAC TFs and the SDOs. Additionally, adopt both the *Proposed NIST Standard for Role-Based Access Control* NIST document and the *A Scenario-driven Role Engineering Process for Functional RBAC Roles* article by G. Neumann and M. Strembeck as advisory materials.

- Identify and assign functional areas and usage scenarios to the various Enterprise RBAC Task Forces. Each Enterprise RBAC TF will identify and define healthcare scenarios when HL7 storyboards do not exist, then model the usage scenarios to define the tasks, permissions and operations for healthcare roles.

- Function as a liaison between the SDO and the Enterprise RBAC TFs.

- Collect and consolidate all information defined by the Enterprise RBAC TFs for development of a set of standard tasks and permissions for the healthcare community. The Healthcare RBAC TF will present this information for use as a recommended standard to an SDO. (The SDO would then turn the information from the Healthcare RBAC TF into a proposed RBAC standard for use within the healthcare community.)

1.3 Healthcare Enterprise Needs

RBAC was developed to overcome the complexities of managing individual user permissions. The Healthcare RBAC efforts are also motivated by the desires to:

- Simplify authorization management,
- Reduce administrative costs,
- Improve security,
- Enhance partner interoperability,
- Enable new network-level RBAC services, and
- Improve service to members/clients/patients.

The healthcare community and standards groups recognize RBAC as a high priority for numerous reasons, including:

- HIPAA security and privacy regulations (confidentiality of electronic patient records)

- National access and control standards,
- Interoperability,
- Data security, and
- System security.

Ultimately, the Healthcare RBAC Task Force and the participating Enterprise Task Forces could establish and influence definitions of industry standards for RBAC permission management for use within the entire healthcare community.

1.4 Work Products

The following table lists the Work Products of the Healthcare RBAC TF.

Table 1: Work Products

Work Product	Description
Healthcare RBAC Task Force Plan	This document will outline the management, activities, communications and risks.
RBAC Task Force Process Document	This document will describe the defined process for analyzing the healthcare workflows and defining the tasks and associated permissions within healthcare roles.
Healthcare RBAC Task List	This work product is a list of tasks and permissions and operations for healthcare roles to be used by an SDO for preparation of a draft healthcare RBAC standard. The Task List is a harmonized collection from the participating RBAC Enterprise Task Forces.

1.5 Healthcare Enterprise Requirements

Following are high-level requirements that the Healthcare RBAC TF shall satisfy include the following:

- The Healthcare RBAC TF will be established as a collaborative unit comprised of healthcare organizations that include DoD, IHS, KP and VA.

- The Healthcare RBAC TF shall promote interoperability between healthcare systems.

- The Healthcare RBAC TF shall coordinate the functional area modeling assignments to the Enterprise RBAC Task Forces.

- The Healthcare RBAC TF shall produce a Healthcare RBAC Task List, which is a harmonized list of Healthcare permissions and associated work profile representations from the participating RBAC Enterprise Task Forces.

- The Healthcare RBAC TF shall submit the Healthcare RBAC Task List to an SDO as a draft healthcare RBAC standard.

1.6 Healthcare RBAC Task Force Exit Criteria

The exit criteria are guideposts to indicate when the task force has met its objectives in a satisfactory manner. Since this is a collaborative effort, the collaboration will need to collectively evaluate the effectiveness of the exit criteria.

The following table provides the goals with respect to the final work product, i.e., the Healthcare RBAC Task List.

Table 2: Exit Criteria

Exit Criteria	Description
Completeness	• Does the goal or work product cover all recognized topics? • Are these topics covered adequately?
Correctness	• Are all parts of the goal or work product free from significant errors?
Internal Consistency	• Are all parts of the goal or work product consistent with each other?
External Consistency	• Are all parts of the goal or work product consistent with other accepted sources?
Generality	• Is the goal or work product free of ad hoc assumptions and locally defined components?
Simplicity	• Are the parts of the goal or work product free of complex language or analysis that may impede the document's use?

1.7 Scope Boundaries

The goal of the Healthcare RBAC TF will be completed when a list of tasks and associated permissions are defined. The HL7 storyboards and domain experts from the Enterprise RBAC Task Forces will provide the business workflows. The Healthcare RBAC TF will provide the SDO with information necessary for the development of a standard. The creation of a healthcare RBAC standard is not within the scope of these activities, but will be developed by the SDO committees.

The definition of roles is not within the scope of the Healthcare RBAC TF. From an interoperability perspective, roles are irrelevant as they are configurable by organization and therefore, are not interoperable at the inter-organizational level. The list of tasks satisfies the interoperability requirements. The TF may, at its discretion, develop a suggested role set.

2 Assurance

2.1 Scope Risk Limit

If all of the exit criteria are not sufficiently met, the Healthcare RBAC Task Force will have produced a less than optimum result. In this case, additional work may be deemed necessary before RBAC can be successfully deployed within healthcare organizations.

This collaborative aspect is itself a risk factor to the success of the Healthcare RBAC TF. Another risk factor will be the level of resources that can be made available to the Healthcare RBAC TF for these activities. Therefore, it will be necessary to assess the accomplishment of the exit criteria on a continual basis. A mid-work product review should be planned to assess the likely outcome of the task force.

2.2 Reviews and Approvals

Management review and approval will occur for this Healthcare RBAC Task Force Charter and the Healthcare RBAC Task Force Plan.

Collaboration review will occur for this charter document, the Healthcare RBAC Task Force Plan, the RBAC Task Force Role Engineering Process document, and the Healthcare RBAC Task List. The Healthcare RBAC Task List will be approved by the collaboration.

2.3 Communications

Status reporting will include formal and informal methods including e-mail, scheduled conference calls, status reports and potential face-to-face meetings.

E-mail. E-mail is used, as needed, for communication between Healthcare RBAC Task Force members. E-mail will not be used to transmit sensitive data.

Groove. The Groove collaboration tool allows users to create secure interactive shared spaces where information, people and tools are all brought together seamlessly. Shared spaces sit on each user's PC. Work done in the space by one 'member' is instantly seen by all members. Groove keeps all members' PCs updated with the latest changes. All Groove data is automatically encrypted, thus protecting privacy and intellectual property. A free version of the software is available at http://www.groove.net.

Conference Calls. Conference calls are scheduled, as necessary, to achieve the goals of the Healthcare RBAC Task Force. Since this organization involves personnel all over the nation, it is anticipated that conference calls will occur frequently.

Status Reports. Status reporting will be achieved through a bi-weekly Healthcare RBAC Task Force conference call. All Task Force members are expected to attend. The RBAC Project Lead will present a summary of current statuses and progress to the assembled team members, addresses current RBAC issues, and answers any questions. An advanced e-mail posting will

provide all documents necessary for review prior to the monthly conference call. Minutes of the call will be prepared and distributed to the Healthcare RBAC Task Force collaboration.

Website. A Healthcare RBAC website will be established and realized as the primary location for all data input, review, and approval. This website will be enabled with mechanisms to ensure proper data access and operations on that data.

3 Resource Limits

3.1 Team composition

Healthcare RBAC TF. This Task Force will consist of representatives from the following organizations:

- Department of Veterans Affairs (VA)
- Department of Defense (DoD)
- Kaiser Permanente (KP)
- Indian Health Service (IHS)

3.2 Deadline

Refer to the Healthcare RBAC TF Plan for a detailed schedule of activities.

3.3 Healthcare RBAC Task Force Constraints

The primary constraints on the TF activities will be schedule and resources. As mentioned in Section 2.1, progress will be continually monitored to mitigate the effects of resource constraints.